

1 1. In a security heterogenic computer network supporting different security
2 descriptor specifications, the computer network having one or more devices that use a first
3 security descriptor that follows a first security descriptor specification to describe security
4 permissions related to a particular object, the computer network also having one or more
5 devices that use a second security descriptor that follows a second security descriptor
6 specification to describe security permissions related to that same particular object, a
7 method of replicating in a non-degenerative fashion the first security descriptor with the
8 second security descriptor specification, the method facilitating the synchronization of the
9 first and second security descriptor specifications so that both security specifications may
10 be used in the computer network, the method comprising the following:

11 a step for converting the first security descriptor that follows the first
12 security descriptor specification into a version of the first security descriptor that
13 follows the second security descriptor specification;

14 a step for comparing the version of the first security descriptor that follows
15 the second security descriptor specification with the second security descriptor that
16 also follows the second security descriptor specification; and

17 an act of changing the second security descriptor to reflect at least some of
18 the changes represented in the version of the first security descriptor.

19
20 2. A method in accordance with Claim 1, wherein the first security descriptor
21 specification is the 4.0 specification.

22
23 3. A method in accordance with Claim 2, wherein the second security
24 descriptor specification is the Active Directory specification.

based on the act of comparing, an act of detecting changes in the first security descriptor that are not reflected in the second security descriptor.

THE UNIVERSITY OF CHICAGO

Sub
ale

WORKMAN, NYDEGGER & SEELEY

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

1000 EAGLE GATE TOWER

60 EAST SOUTH TEMPLE

SALT LAKE CITY, UTAH 84111

OFFICE

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

8. In a security heterogenic computer network supporting different security descriptor specifications, the computer network having one or more devices that use a first security descriptor that follows a first security descriptor specification to describe security permissions related to a particular object, the computer network also having one or more devices that use a second security descriptor that follows a second security descriptor specification to describe security permissions related to that same particular object, a method of replicating in a non-degenerative fashion the first security descriptor with the second security descriptor specification, the method facilitating the synchronization of the first and second security descriptor specifications so that both security specifications may be used in the computer network, the method comprising the following:

an act of consulting mapping rules that define mappings of rights of the first security descriptor specification to rights of the second security descriptor specification;

for each right for which there is a corresponding mapping rule, converting the right that follows the first security descriptor specification to a corresponding right that follows the second security descriptor specification;

an act of assembling each corresponding right that follows the second security descriptor specification to form a version of the first security descriptor that follows the second security descriptor specification;

for each right for which there is a corresponding mapping rule, an act of comparing the right in the version of the first security descriptor that follows the second security descriptor specification to the right in the second security descriptor;

12. A method in accordance with Claim 11, wherein the second security descriptor specification is the 4.0 specification.

13. A computer program product for use in a security heterogenic computer network supporting different security descriptor specifications, the computer network having one or more devices that use a first security descriptor that follows a first security descriptor specification to describe security permissions related to a particular object, the computer network also having one or more devices that use a second security descriptor that follows a second security descriptor specification to describe security permissions related to that same particular object, the computer program product for implementing a method of replicating in a non-degenerative fashion the first security descriptor with the second security descriptor specification, the method facilitating the synchronization of the first and second security descriptor specifications so that both security specifications may be used in the computer network, the computer program product comprising a computer-readable medium having computer-executable instructions for performing the following:

a step for converting the first security descriptor that follows the first security descriptor specification into a version of the first security descriptor that follows the second security descriptor specification;

a step for comparing the version of the first security descriptor that follows the second security descriptor specification with the second security descriptor that also follows the second security descriptor specification; and

an act of changing the second security descriptor to reflect at least some of the changes represented in the version of the first security descriptor.

14. A computer program product in accordance with Claim 13, wherein the first security descriptor specification is the 4.0 specification.

Sub
ale

15. A computer program product in accordance with Claim 14, wherein the second security descriptor specification is the Active Directory specification.

16. A computer program product in accordance with Claim 14, wherein the first security descriptor specification is the Active Directory specification.

17. A computer program product in accordance with Claim 16, wherein the second security descriptor specification is the 4.0 specification.

18. A computer program product in accordance with Claim 13, wherein the computer-executable instructions for performing the step for converting the first security descriptor that follows the first security descriptor specification into a version of the first security descriptor that follows the second security descriptor specification comprise computer-executable instructions for performing the following:

an act of consulting mapping rules that define mappings of rights of the first security descriptor specification to rights of the second security descriptor specification;

for each right for which there is a corresponding mapping rule, converting the right that follows the first security descriptor specification to a corresponding right that follows the second security descriptor specification; and

an act of assembling each corresponding right that follows the second security descriptor specification to form a version of the first security descriptor that follows the second security descriptor specification.

based on the act of comparing, an act of detecting changes in the first security descriptor that are not reflected in the second security descriptor.

Sub
all

1 20. A computer program product for use in a security heterogenic computer
2 network supporting different security descriptor specifications, the computer network
3 having one or more devices that use a first security descriptor that follows a first security
4 descriptor specification to describe security permissions related to a particular object, the
5 computer network also having one or more devices that use a second security descriptor
6 that follows a second security descriptor specification to describe security permissions
7 related to that same particular object, a computer program product for implementing a
8 method of replicating in a non-degenerative fashion the first security descriptor with the
9 second security descriptor specification, the method facilitating the synchronization of the
10 first and second security descriptor specifications so that both security specifications may
11 be used in the computer network, the computer program product comprising a computer-
12 readable medium having computer-executable instructions for performing the following:

13 an act of consulting mapping rules that define mappings of rights of the first
14 security descriptor specification to rights of the second security descriptor
15 specification;

16 for each right for which there is a corresponding mapping rule, converting
17 the right that follows the first security descriptor specification to a corresponding
18 right that follows the second security descriptor specification;

19 an act of assembling each corresponding right that follows the second
20 security descriptor specification to form a version of the first security descriptor
21 that follows the second security descriptor specification;

22 for each right for which there is a corresponding mapping rule, an act of
23 comparing the right in the version of the first security descriptor that follows the
24

based on the act of comparing, an act of detecting changes in the first security descriptor that are not reflected in the second security descriptor; and

an act of changing the second security descriptor to reflect the detected changes in the first security descriptor.

22. A computer program product in accordance with Claim 21, wherein the second security descriptor specification is the Active Directory specification.

24. A computer program product in accordance with Claim 23, wherein the second security descriptor specification is the 4.0 specification.

Sub
ale

25. A computer system comprising the following:

a processing device; and

a combination of one or more computer-readable media which in combination have stored thereon the following:

a first data structure that represents a first security descriptor that follows a first security descriptor specification and that represents an object;

a second data structure that represents a second security descriptor that follows a second security descriptor specification and that also represents the object;

a third data structure that represent mapping rules that correlate sets of one or more rights of the first security descriptor specification which sets of one or more rights of the second security descriptor specification; and

computer-executable instruction that, when executed by the processor, perform the following:

a step for converting the first security descriptor that follows the first security descriptor specification into a version of the first security descriptor that follows the second security descriptor specification;

a step for comparing the version of the first security descriptor that follows the second security descriptor specification with the second security descriptor that also follows the second security descriptor specification; and

CONFIDENTIAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

Sub
Ale

an act of changing the second security descriptor to reflect at least some of the changes represented in the version of the first security descriptor.

See
ac

- 1 26. A computer-readable medium having stored thereon the following:
- 2 a first data structure that represents a first security descriptor that follows a
- 3 first security descriptor specification and that represents an object;
- 4 a second data structure that represents a second security descriptor that
- 5 follows a second security descriptor specification and that also represents the
- 6 object;
- 7 a third data structure that represent mapping rules that correlate sets of one
- 8 or more rights of the first security descriptor specification which sets of one or
- 9 more rights of the second security descriptor specification; and
- 10 a fourth data structure that represents a version of the first security
- 11 descriptor that follows the second security descriptor specification.
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24